EEC173B/ECS152C, Winter 2006

Mobile Ad Hoc Networks (MANET)

- Introduction
- Unicast Routing

Acknowledgment: Selected slides from Prof. Nitin Vaidya

Mobile Ad Hoc Networks (MANET)

Properties

- Formed by wireless hosts which may be mobile
- Without (necessarily) using a pre-existing infrastructure
- Routes between nodes may potentially contain multiple hops

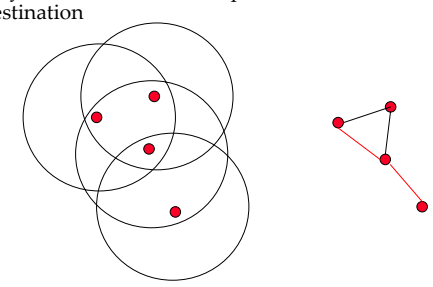
Why?

- Ease of deployment
- Speed of deployment
- Decreased dependence on infrastructure

2

Mobile Ad Hoc Networks

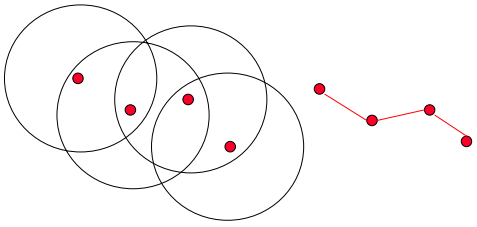
- May need to traverse multiple links to reach a destination



3

Mobile Ad Hoc Networks (MANET)

- Mobility causes route changes



4

Many Applications

- Personal area networking
  - Cell phone, laptop, ear phone, wrist watch
- Military environments
  - Soldiers, tanks, planes
- Civilian environments
  - Taxi cab network
  - Meeting rooms
  - Sports stadiums
  - Boats, small aircraft
- Emergency operations
  - Search-and-rescue
  - Policing and fire fighting

5

Many Variations (1)

- Fully Symmetric Environment
  - All nodes have identical capabilities and responsibilities
- Asymmetric Capabilities
  - Transmission ranges and radios may differ
  - Battery life at different nodes may differ
  - Processing capacity may be different at different nodes
  - Speed of movement
- Asymmetric Responsibilities
  - Only some nodes may route packets
  - Some nodes may act as leaders of nearby nodes (e.g., cluster head)

6

Many Variations (2)

- Traffic characteristics may differ in different ad hoc networks
  - Bit rate
  - Timeliness constraints
  - Reliability requirements
  - Unicast / multicast / geocast
  - Host-based addressing / content-based addressing / capability-based addressing
- May co-exist (and co-operate) with an infrastructure-based network

7

Many Variations (3)

- Mobility patterns may be different
  - People sitting at an airport lounge
  - New York taxi cabs
  - Kids playing
  - Military movements
  - Personal area network
- Mobility characteristics
  - Speed
  - Predictability
    - Direction of movement
    - Pattern of movement
  - Uniformity (or lack thereof) of mobility characteristics among different nodes

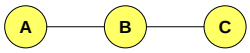
8

Challenges

- Limited wireless transmission range
- Broadcast nature of the wireless medium
  - Hidden terminal problem (see next slide)
- Packet losses due to transmission errors
- Mobility-induced route changes
- Mobility-induced packet losses
- Battery constraints
- Potentially frequent network partitions
- Ease of snooping on wireless transmissions (security hazard)

9

Hidden Terminal Problem



Nodes A and C cannot hear each other

Transmissions by nodes A and C can collide at node B

Nodes A and C are hidden from each other

10

Research on MANET

Variations in capabilities & responsibilities

X

Variations in traffic characteristics, mobility models, etc.

X

Performance criteria (e.g., optimize throughput, reduce energy consumption)

+

Increased research funding

=

Significant research activity

11

The Holy Grail

- A one-size-fits-all solution
  - Perhaps using an adaptive/hybrid approach that can adapt to situation at hand
- Difficult problem
- Many solutions proposed trying to address a sub-space of the problem domain

Assumptions

- Unless stated otherwise, fully symmetric environment is assumed implicitly
  - all nodes have identical capabilities and responsibilities

12

Why is Routing in MANET different ?

- Host mobility
  - link failure/repair due to mobility may have different characteristics than those due to other causes
- Rate of link failure/repair may be high when nodes move fast
- New performance criteria may be used
  - route stability despite mobility
  - energy consumption

13

Unicast Routing Protocols

- Many protocols have been proposed
- Some have been invented specifically for MANET
- Others are adapted from previously proposed protocols for wired networks
- No single protocol works well in all environments
  - Some attempts made to develop adaptive protocols

14

Classification of Routing Protocols

- Proactive protocols
  - Determine routes independent of traffic pattern
  - Traditional link-state and distance-vector routing protocols are proactive
- Reactive protocols
  - Maintain routes only if needed
- Hybrid protocols
- Topology-based vs. Position-based (geographical)
  - Traditional link-state and distance-vector are topology-based => learn about adjacencies with neighboring nodes
  - Position-based use geographical location (e.g., nodes with GPS receiver) to make routing decision, e.g., forward to nodes that are "closer" to destination

15

Trade-Off

- Latency of route discovery
  - Proactive protocols may have lower latency since routes are maintained at all times
  - Reactive protocols may have higher latency because a route from X to Y will be found only when X attempts to send to Y
- Overhead of route discovery/maintenance
  - Reactive protocols may have lower overhead since routes are determined only if needed
  - Proactive protocols can (but not necessarily) result in higher overhead due to continuous route updating
- Which approach achieves a better trade-off depends on the traffic and mobility patterns (and hence, topology)

16

Overview of Unicast Routing Protocols

Reactive Protocols

- Flooding
- DSR
- LAR
- AODV

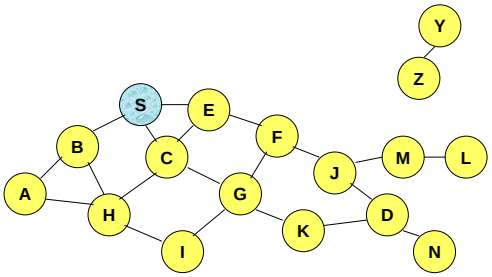
Most well-known MANET routing protocols

Flooding for Data Delivery

- Sender S broadcasts data packet P to all its neighbors
- Each node receiving P forwards P to its neighbors
- Sequence numbers used to avoid the possibility of forwarding the same packet more than once
- Packet P reaches destination D provided that D is reachable from sender S
- Node D does not forward the packet

18

Flooding for Data Delivery



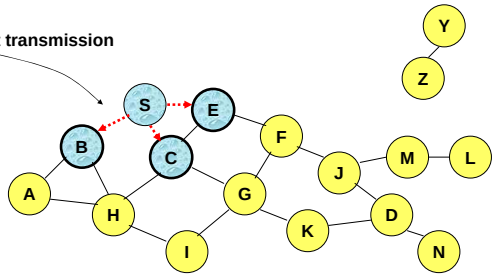
Represents a node that has received packet P

Represents that connected nodes are within each other's transmission range

19

Flooding for Data Delivery

Broadcast transmission

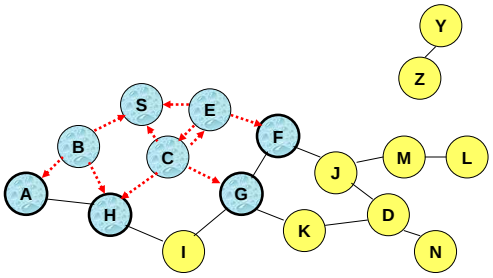


Represents a node that receives packet P for the first time

Represents transmission of packet P

20

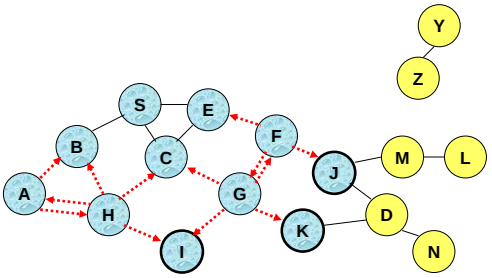
Flooding for Data Delivery



- Node H receives packet P from two neighbors:
  potential for collision

21

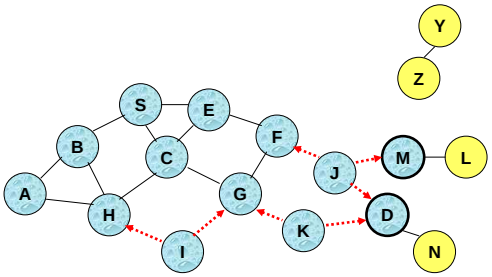
Flooding for Data Delivery



- Node C receives packet P from G and H, but does not forward it again, because node C has already forwarded packet P once

22

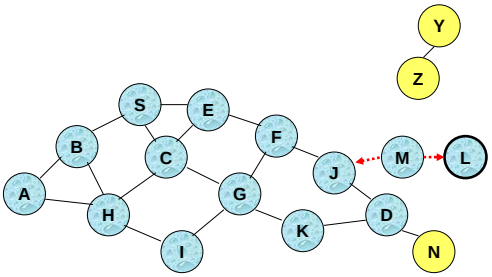
Flooding for Data Delivery



- Nodes J and K both broadcast packet P to node D
- Since nodes J and K are hidden from each other, their transmissions may collide
  => Packet P may not be delivered to node D at all, despite the use of flooding

23

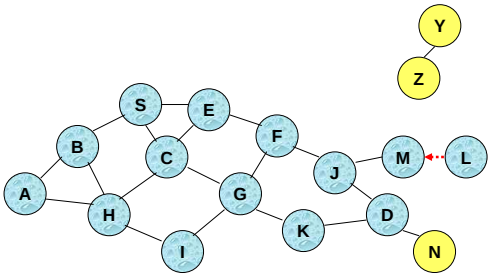
Flooding for Data Delivery



- Node D does not forward packet P, because node D is the intended destination of packet P

24

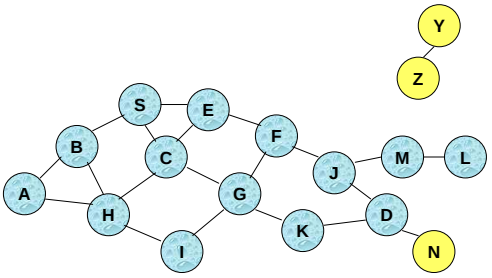
Flooding for Data Delivery



- Flooding completed
- Nodes unreachable from S do not receive packet P (e.g., node Z)
- Nodes for which all paths from S go through the destination D also do not receive packet P (example: node N)

25

Flooding for Data Delivery



- Flooding may deliver packets to too many nodes (in the worst case, all nodes reachable from sender may receive the packet)

26

Flooding: Advantages

- Simplicity
- May be more efficient than other protocols when rate of information transmission is low enough that the overhead of explicit route discovery/maintenance incurred by other protocols is relatively higher
  - This scenario may occur, for instance, when nodes transmit small data packets relatively infrequently, and many topology changes occur between consecutive packet transmissions
- Potentially higher reliability of data delivery
  - Because packets may be delivered to the destination on multiple paths

27

Flooding: Disadvantages

- Potentially, very high overhead
  - Data packets may be delivered to too many nodes who do not need to receive them
- Potentially lower reliability of data delivery
  - Flooding uses broadcasting -- hard to implement reliable broadcast delivery without significantly increasing overhead
    - Broadcasting in IEEE 802.11 MAC is unreliable
  - In our example, nodes J and K may transmit to node D simultaneously, resulting in loss of the packet
    - In this case, destination would not receive the packet at all

28

Flooding of Control Packets

- Many protocols perform (potentially *limited*) flooding of control packets, instead of data packets
- The control packets are used to discover routes
- Discovered routes are subsequently used to send data packet(s)
- Overhead of control packet flooding is amortized over data packets transmitted between consecutive control packet floods

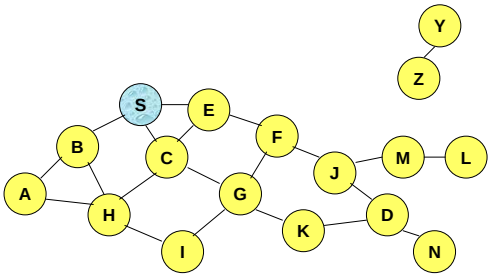
29

Dynamic Source Routing (DSR)

- [Johnson96] David B. Johnson and David A. Maltz. Dynamic Source Routing in Ad Hoc Wireless Networks. In *Mobile Computing*, edited by Tomasz Imielinski and Hank Korth, Chapter 5, pages 153-181, Kluwer Academic Publishers, 1996.
- When node S wants to send a packet to node D, but does not know a route to D, node S initiates a route discovery
- Source node S floods Route Request (RREQ)
- Each node appends own identifier when forwarding RREQ

30

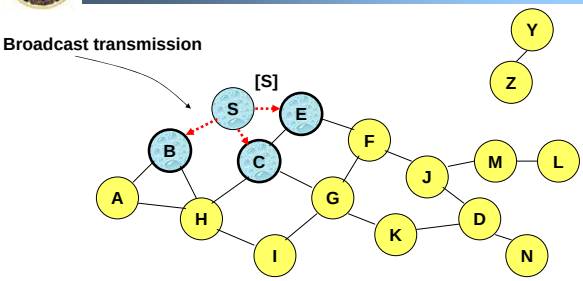
Route Discovery in DSR



Represents a node that has received RREQ for D from S

31

Route Discovery in DSR

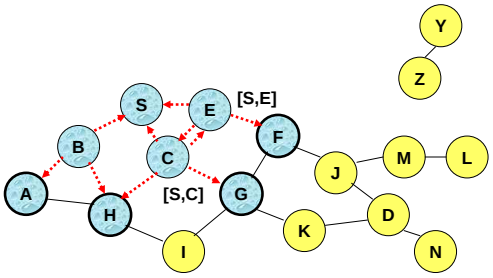


Represents transmission of RREQ

[X,Y] Represents list of identifiers appended to RREQ

32

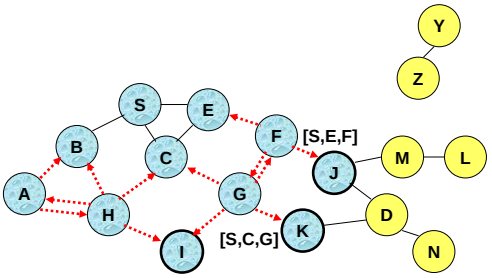
Route Discovery in DSR



- Node H receives packet RREQ from two neighbors: potential for collision

33

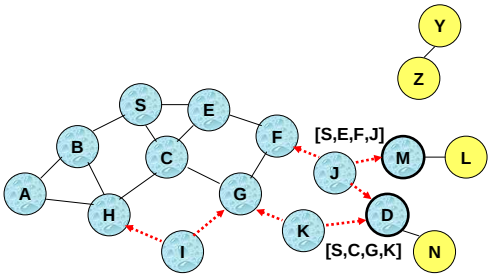
Route Discovery in DSR



- Node C receives RREQ from G and H, but does not forward it again, because node C has already forwarded RREQ once

34

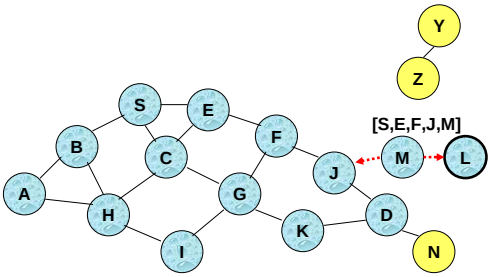
Route Discovery in DSR



- Nodes J and K both broadcast RREQ to node D
- Since nodes J and K are hidden from each other, their transmissions may collide

35

Route Discovery in DSR



- Node D does not forward RREQ, because node D is the intended target of the route discovery

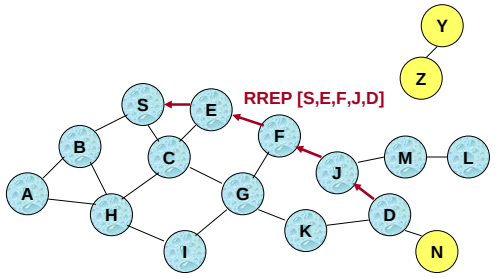
36

Route Discovery in DSR

- Destination D on receiving the first RREQ, sends a Route Reply (RREP)
- RREP is sent on a route obtained by reversing the route appended to received RREQ
- RREP includes the route from S to D on which RREQ was received by node D

37

Route Reply in DSR



Represents RREP control message

38

Route Reply in DSR

- Route Reply can be sent by reversing the route in Route Request (RREQ) only if links are guaranteed to be bi-directional
  - To ensure this, RREQ should be forwarded only if it received on a link that is known to be bi-directional
- If unidirectional (asymmetric) links are allowed, then RREP may need a route discovery for S from node D
  - Unless node D already knows a route to node S
  - If a route discovery is initiated by D for a route to S, then the Route Reply is piggybacked on the Route Request from D.
- If IEEE 802.11 MAC is used to send data, then links have to be bi-directional (since Ack is used)

39

Dynamic Source Routing (DSR)

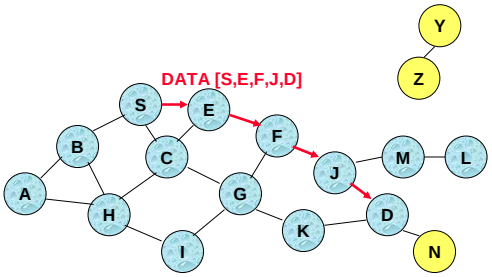
- Node S on receiving RREP, caches the route included in the RREP
- When node S sends a data packet to D, the entire route is included in the packet header
  - Hence the name source routing
- Intermediate nodes use the source route included in a packet to determine to whom a packet should be forwarded

When to Perform a Route Discovery?

- When node S wants to send data to node D, but does not know a valid route node D

40

Data Delivery in DSR



Packet header size grows with route length

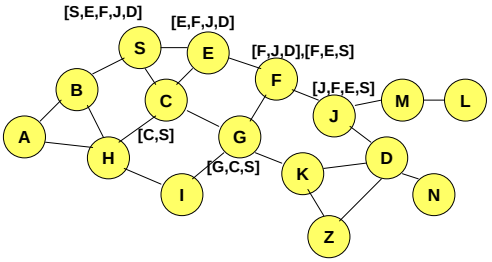
DSR Optimization: Route Caching

- Each node caches a new route it learns by *any means*
- When node S finds route [S,E,F,J,D] to node D, node S also learns route [S,E,F] to node F
- When node K receives Route Request [S,C,G] destined for node D, node K learns route [K,G,C,S] to node S
- When node F forwards Route Reply RREP [S,E,F,J,D], node F learns route [F,J,D] to node D
- When node E forwards Data [S,E,F,J,D] it learns route [E,F,J,D] to node D
- A node may also learn a route when it overhears Data packets

Use of Route Caching

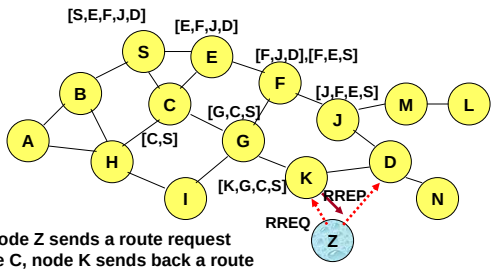
- When node S learns that a route to node D is broken, it uses another route from its local cache, if such a route to D exists in its cache. Otherwise, node S initiates route discovery by sending a route request
- Node X on receiving a Route Request for some node D can send a Route Reply if node X knows a route to node D
- Use of route cache
  - Can speed up route discovery
  - Can reduce propagation of route requests

Use of Route Caching



[X,X,X] Represents cached route at a node
(DSR maintains the cached routes in a tree format)

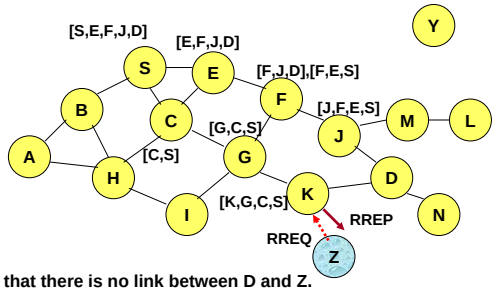
Use of Route Caching: Can Speed up Route Discovery



When node Z sends a route request for node C, node K sends back a route reply [Z,K,G,C] to node Z using a locally cached route

45

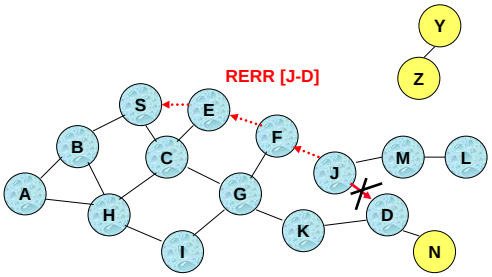
Use of Route Caching: Can Reduce Propagation of Route Requests



Assume that there is no link between D and Z.
Route Reply (RREP) from node K limits flooding of RREQ.
In general, the reduction may be less dramatic.

46

Route Error (RERR)



J sends a route error to S along route J-F-E-S when its attempt to forward the data packet S (with route SEFJD) on J-D fails

Nodes hearing RERR update their route cache to remove link J-D

47

Route Caching: Beware!

- Stale caches can adversely affect performance
- With passage of time and host mobility, cached routes may become invalid
- A sender host may try several stale routes (obtained from local cache, or replied from cache by other nodes), before finding a good route

48

DSR: Advantages

- Routes maintained only between nodes who need to communicate
  - reduces overhead of route maintenance
- Route caching can further reduce route discovery overhead
- A single route discovery may yield many routes to the destination, due to intermediate nodes replying from local caches

49

DSR: Disadvantages

- Packet header size grows with route length due to source routing
- Flood of route requests may potentially reach all nodes in the network
- Care must be taken to avoid collisions between route requests propagated by neighboring nodes
  - insertion of random delays before forwarding RREQ
- Increased contention if too many route replies come back due to nodes replying using their local cache
  - Route Reply *Storm* problem
  - Reply storm may be eased by preventing a node from sending RREP if it hears another RREP with a shorter route

50

DSR: Disadvantages

- An intermediate node may send Route Reply using a stale cached route, thus polluting other caches
- This problem can be eased if some mechanism to purge (potentially) invalid cached routes is incorporated.
- For some proposals for cache invalidation, see [Hu00Mobicom]
  - Static timeouts
  - Adaptive timeouts based on link stability

51